Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application:

Listing of Claims:

1. (Currently Amended) An architecture for confirming the identity of a message sender on a remote services system, comprising:

a communications module operable to transmit a message, wherein said message comprise both forward and back channel messages;

a cryptographic module in said communication module for signing said message and for providing encryption of a data stream in said message when transmission of said message is not via ~~, said cryptographic module comprising~~ secure socket[[s]] layer encryption;

a mid-level manager operating in said remote services system in conjunction with said communications module for controlling the flow of messages in said remote services system between a customer proxy and an applications server and for verifying the identity of a sender by comparing first and second data identities in said data stream, wherein said first data identity comprises data in a network software layer, said second data identity comprises data in an application software layer.

2. (Canceled)

3. (Canceled)

4. (Canceled)

5. (Previously Presented) The architecture according to claim 1, wherein said mid-level manager is a customer mid-level manager.

6. (Previously Presented) The architecture according to claim 1, wherein said mid-level manager is an aggregation mid-level manager.

7. (Previously Presented) The architecture according to claim 1, wherein transmission of said message is conditioned on HTTP.

8. (Previously Presented) The architecture according to claim 1, wherein transmission of said message is conditioned on email protocol.

9. (Currently Amended) A method of confirming the identity of a message sender on a remote services system, comprising:

obtaining a first identity related to a message, said first identity being obtained from a network software layer in said remote services system wherein said first identity is extracted from a secure socket layer transmission or a digital signature of said message;

subsequent to obtaining the first identity, obtaining a second identity related to the sender of [[a]]said message[[s]], said second identity being obtained from an application software layer in said remote services system; and

comparing at a mid-level manager, wherein said mid-level manager operates in said remote services system in conjunction with a communications module for controlling the flow of messages in said remote services system between a customer proxy and an applications server and in conjunction with an intermediate mid-level manager that provides data queue management, transaction integrity and redundancy, said first identity with said second identity to verify the identity of the sender of said message.

10. (Canceled)

11. (previously presented) The method according to claim 9, further comprising encrypting said message and said identities in an encryption module in said remote services system.

12. (Original) The method according to claim 11, said encryption of said data and said identities being performed in accordance with secure socket layer protocol.

13. (Original) The method according to claim 12, said message being transmitted in said system using HTTP protocol.

14. (Original) The method according to claim 12, said message being transmitted in said system using email protocol.

15. (Currently amended) A method of confirming the identity of a message sender on a remote services system, comprising:

transmitting a message using a communications module of said remote services system;

encrypting a data stream in said message using an encryption module in said communications module, said encryption module comprising secure sockets layer encryption[[: and]];

determining whether said message is transmitted using secure socket layer encryption;

responsive to secure socket layer encryption being used, extracting a first identity;

responsive to the absence of use of secure socket layer encryption, extracting the first identity by decrypting and verifying a signature of the message sender;

controlling the flow of said message between a customer proxy and an applications server in said remote services system using a mid-level manager, said mid-level manager verifying the identity of a sender by comparing first and second data identities in said data stream, wherein said first identity comprises encrypted data in a network software layer of said remote services system, said second identity comprises encrypted data in an application software layer of said remote services system.

16. (Canceled)

17. (Canceled)

18. (Canceled)

19. (Original) The method according to claim 15, wherein said mid-level manager is a customer mid-level manager.

20. (Original) The method according to claim 15, wherein said mid-level manager is an aggregation mid-level manager.

21. (Previously presented) The architecture according to claim 1, wherein said mid-level manager operates in conjunction with an intermediate mid-level manager that provides data queue management, transaction integrity and redundancy.

22. (Previously presented) The method according to claim 15, wherein said mid-level manager operates in conjunction with an intermediate mid-level manager that provides data queue management, transaction integrity and redundancy.